PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-075597
(43)Date of publication of application : 26.03.1993

(51)Int.Cl. H04L 9/06
H04L 9/14
G09C 1/00

(21)Application number : 03-230580
(22)Date of filing : 10.09.1991

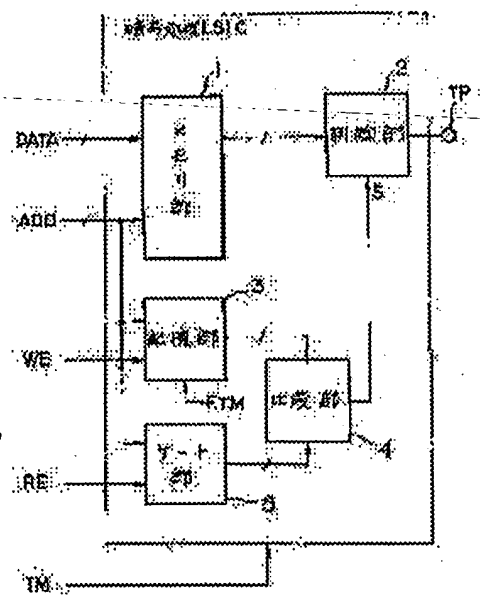
(71)Applicant : FUJITSU LTD
(72)Inventor : TANAKA HIDEAKI

(54) SECRET KEY PROTECTING SYSTEM AND CIPHER PROCESSING LSIC BY THIS SYSTEM

(57)Abstract:

PURPOSE: To provide the secret key protecting system and the cipher processing of this system where read/write of a memory part where secret key data is stored can be checked but secret key data cannot be observed from the external.

CONSTITUTION: Data in a memory part 1 where secret key information is stored can be read/written from the external in the test mode. A control part 2 which controls permission/inhibition of external output of read data from the memory part 1, a storage part 3 where all stored information are reset by input of a test mode signal TM and information related to addresses where data is written in the memory part 1 is stored thereafter, and a comparing part 4 which compares stored information of the storage part 3 and information related to the address for data read of the memory part 1 with each other are provided. When the test mode is set and the comparison in the comparing part 4 results in coincidence, the control part 2 permits data output. The memory part 1 and a cipher processing part which generates secret key information are unified and integrated into a cipher processing LSIC to improve the secrecy.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision

of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平5－75597

(43)公開日　平成5年(1993)3月26日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/06					
	9/14					
Ｇ０９Ｃ	1/00		9194－5Ｌ			
			7117－5Ｋ	Ｈ０４Ｌ	9/02	Ｚ

審査請求　未請求　請求項の数2(全　8　頁)

(21)出願番号　特願平3－230580

(22)出願日　平成3年(1991)9月10日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地
(72)発明者　田中　秀明
宮城県仙台市青葉区一番町１丁目２番25号
富士通東北デイジタル・テクノロジ株式会社内
(74)代理人　弁理士　井桁　貞一

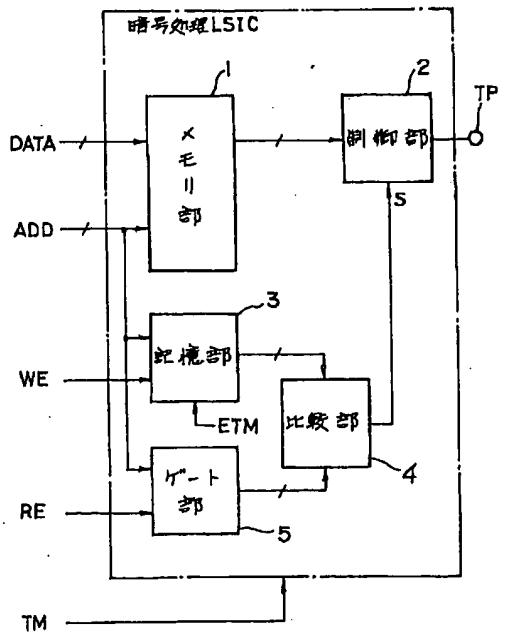
(54)【発明の名称】　秘密鍵保護方式及び該方式による暗号処理ＬＳＩＣ

(57)【要約】

【目的】　本発明は秘密鍵保護方式及び該方式による暗号処理ＬＳＩＣに関し、秘密鍵データを記憶するメモリ部の読み／書き検査が可能であると共に外部からは秘密鍵データを観測できない秘密鍵保護方式及び該方式による暗号処理ＬＳＩＣの提供を目的とする。

【構成】　テストモードにより秘密鍵情報を記憶するメモリ部１のデータを外部から読み／書き可能に構成された装置の秘密鍵保護方式において、メモリ部１の読出データの外部出力可否を制御する制御部２と、テストモード信号ＴＭの投入により全記憶情報がリセットされて、その後のメモリ部１へのデータ書込を行ったアドレスに係る情報を記憶する記憶部３と、記憶部３の記憶情報とメモリ部１のデータ読出を行うアドレスに係る情報とを比較する比較部４とを備え、テストモードでかつ比較部４の比較一致が得られたことにより制御部２を出力可にする。またメモリ部１と秘密鍵情報を発生する暗号処理部とを一体化、集積化して暗号処理ＬＳＩＣとなし、秘匿性を向上させる。

本発明の原理的構成図



1

【特許請求の範囲】

【請求項1】　テストモードにより、秘密鍵に係る情報を記憶するメモリ部（1）のデータを外部から読み／書き可能に構成された装置の秘密鍵保護方式において、

メモリ部（1）の読出データの外部への出力可否を制御する制御部（2）と、

テストモード信号（TM）の投入により全記憶情報がリセットされて、その後のメモリ部（1）へのデータの書き込みを行ったアドレスに係る情報を記憶する記憶部（3）と、

記憶部（3）の記憶情報とメモリ部（1）のデータの読み出しを行うアドレスに係る情報とを比較する比較部（4）とを備え、

テストモードでかつ比較部（4）の比較一致が得られたことにより制御部（2）を出力可にすることを特徴とする秘密鍵保護方式。

【請求項2】　テストモードにより、秘密鍵に係る情報を記憶するメモリ部（1）のデータを外部から読み／書き可能に構成された記憶装置を備える暗号処理ＬＳＩＣにおいて、

メモリ部（1）の読出データの外部端子（ＴＰ）への出力可否を制御する制御部（2）と、

テストモード信号（TM）の投入により全記憶情報がリセットされて、その後のメモリ部（1）へのデータの書き込みを行ったアドレスに係る情報を記憶する記憶部（3）と、

記憶部（3）の記憶情報とメモリ部（1）のデータの読み出しを行うアドレスに係る情報とを比較する比較部（4）とを備え、

テストモードでかつ比較部（4）の比較一致が得られたことにより制御部（2）を出力可にするように構成されたことを特徴とする暗号処理ＬＳＩＣ。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は秘密鍵保護方式及び該方式による暗号処理ＬＳＩＣに関し、更に詳しくは、テストモードにより、秘密鍵に係る情報を記憶するメモリ部のデータを外部から読み／書き可能に構成され装置の秘密鍵保護方式及び該方式による暗号処理ＬＳＩＣに関する。

【０００２】近年、社会の高度情報化に伴い、データのセキュリティ保護が強く望まれており、暗号処理の重要性が高まっている。従って、かかる暗号処理の中枢を担う秘密鍵情報を記憶する装置又はこれに暗号処理部を一体化して集積化した暗号処理ＬＳＩＣにおいては、鍵データの秘密管理が極めて重要であり、仮に、このＬＳＩＣ等を搭載した装置が盗まれて、動作が解析されようとしても、秘密の鍵データが外部に取り出せないことが重要である。

【０００３】

2

【従来の技術】図４は従来の暗号処理ＬＳＩＣのブロック図で、図において、１０は移動通信端末に組み込まれた暗号処理ＬＳＩＣ、１１はＮＴＴのＦＥＡＬ－８暗号アルゴリズムに従う鍵処理部、１２はセレクタ部、１３はメモリ部、１４は同ＦＥＡＬ－８暗号アルゴリズムに従うデータランダム化部、１５はトライステートのバッファ回路である。

【０００４】通常の動作モードでは、テストモード信号ＴＭはＬＯＷレベルであり、これによってセレクタ部１２は入力端子のＡ側を選択し、かつバッファ回路１５の出力ＴＰはハイインピーダンスである。この状態で、予め、基地局からは６４ビット長の鍵データＫＤが秘密に送られる。鍵処理部１１は、この鍵データＫＤをＦＥＡＬ－８暗号アルゴリズムに従って混ぜ合わせることで暗号強度を増した２５６ビット長の拡大鍵データＥＫＤを生成し、これをメモリ部１３に格納する。

【０００５】次に、基地局又は移動通信端末内の不図示のＣＰＵから６４ビット長の平文データＭＤが送られる。データランダム化部１４は、この平文データＭＤとメモリ部１３の拡大鍵データＥＫＤとをＦＥＡＬ－８暗号アルゴリズムに従って混ぜ合わせることでさらに暗号強度を増した暗号データＣＤを生成し、これを外部に出力する。そして、図示しないが、外部においてサンプリング量子化された音声データは、データランダム化部１４の暗号データＣＤによって暗号化され、無線送信される。

【０００６】ところで、このようなＦＥＡＬ－８暗号アルゴリズムは一般に公開されるものである。しかも、同一の暗号処理ＬＳＩＣが多く市場に出回るので、誰でも入手可能になる。従って、このようなＬＳＩＣを搭載した装置が盗まれた場合には、暗号化動作が解析されてしまうという恐れが生じる。しかし、仮に平文データＭＤが知られてしまっても、拡大鍵データＥＫＤが知られない限りは音声データを復号化できない。しかも、おお元の鍵データＫＤは秘密に送られるものであり、この鍵データＫＤを知らない限りは拡大鍵データＥＫＤを生成できない。従って、このような暗号処理ＬＳＩＣを使用した暗号処理システムは一見安全である。

【０００７】しかるに、一般に、この種の暗号処理ＬＳＩＣではメモリ部１３の記憶動作が正常に行われるか否かを調べる必要があり、このためにメモリ部１３のデータ読み書きをテストするテストモードが設けられている。このテストモードでは、テストモード信号ＴＭはＨＩＧＨレベルであり、これによってセレクタ部１２は入力端子のＢ側を選択し、かつバッファ回路１５の出力はその入力に応じて変化する。即ち、テストモードでは、外部から任意のアドレスＴＡにテストデータＴＤを書き込み、あるいは任意のアドレスＴＡのデータをテスト端子ＴＰに読み出すことが可能である。従って、従来の暗号処理ＬＳＩＣでは、テストモード信号ＴＭをＨＩＧＨ

レベルにすることで秘密の拡大鍵データＥＫＤを容易に知ることができた。

【０００８】

【発明が解決しようとする課題】上記のように従来の暗号処理ＬＳＩＣでは、該ＬＳＩＣをテストモードにすることにより外部から容易に秘密の拡大鍵データを観測できるので、通信を盗聴される恐れがあった。本発明の目的は、外部から秘密鍵データを記憶するメモリ部の読み／書き検査が可能であると共に、外部からは秘密鍵データが観測できない秘密鍵保護方式及び該方式による暗号処理ＬＳＩＣを提供することにある。

【０００９】

【課題を解決するための手段】上記の課題は図１の構成により解決される。即ち、本発明の秘密鍵保護方式は、テストモードにより、秘密鍵に係る情報を記憶するメモリ部１のデータを外部から読み／書き可能に構成された装置の秘密鍵保護方式において、メモリ部１の読出データの外部への出力可否を制御する制御部２と、テストモード信号ＴＭの投入により全記憶情報がリセットされて、その後のメモリ部１へのデータの書き込みを行ったアドレスに係る情報を記憶する記憶部３と、記憶部３の記憶情報とメモリ部１のデータの読み出しを行うアドレスに係る情報とを比較する比較部４とを備え、テストモードでかつ比較部４の比較一致が得られたことにより制御部２を出力可にするものである。

【００１０】また、本発明の暗号処理ＬＳＩＣは、テストモードにより、秘密鍵に係る情報を記憶するメモリ部１のデータを外部から読み／書き可能に構成された記憶装置を備える暗号処理ＬＳＩＣにおいて、メモリ部１の読出データの外部端子ＴＰへの出力可否を制御する制御部２と、テストモード信号ＴＭの投入により全記憶情報がリセットされて、その後のメモリ部１へのデータの書き込みを行ったアドレスに係る情報を記憶する記憶部３と、記憶部３の記憶情報とメモリ部１のデータの読み出しを行うアドレスに係る情報とを比較する比較部４とを備え、テストモードでかつ比較部４の比較一致が得られたことにより制御部２を出力可にするように構成されている。

【００１１】

【作用】本発明の秘密鍵保護方式においては、テストモード信号ＴＭの投入によりそのエッジ信号ＥＴＭで記憶部３の全記憶内容がリセットされる。そして、その後にメモリ部１に対して何らかのテストデータＤＡＴＡの書き込みを行うと、その際の書込イネーブル信号ＷＥによってその際の書込アドレスＡＤＤに係る情報が記憶部３に記憶される。こうして、メモリ部１の任意アドレスＡＤＤに任意データＤＡＴＡを書き込むことが可能であり、各書込毎にその書込アドレスＡＤＤに係る情報が記憶部３に記憶される。

【００１２】また、このテストモードでメモリ部１に対してデータＤＡＴＡの読み出しを行うと、ゲート部５はその際の読出イネーブル信号ＲＥによってその際の読出アドレスＡＤＤに係る情報を出力する。そして、比較部４は記憶部３の書込アドレスに係る情報とゲート部５の読出アドレスに係る情報とを比較しており、比較の一致が得られると制御部２を出力可にし、それ以外は出力不可にする。

【００１３】従って、テストモードへの投入後は、メモリ部１に何らかのデータを書き込んだ場合はそのアドレスのデータを外部ＴＰに読み出せるが、データを書き込まなかったアドレスのデータ、即ち、秘密鍵に係るデータは外部ＴＰには読み出せない。かくして、本発明によれば、暗号処理ＬＳＩＣをテストモードにすることによりメモリ部１の読み／書き検査を行うことは可能であるが、秘密の鍵データを外部に読み出すことはできない。

【００１４】また本発明の暗号処理ＬＳＩＣにおいては、テストモードにより、秘密鍵に係る情報を記憶するメモリ部１のデータを外部から読み／書き可能に構成された記憶装置と、この秘密鍵に係る情報を生成等する暗号処理部とを一体化、集積化することで暗号処理装置の秘匿性を一層高めている。

【００１５】

【実施例】以下、添付図面に従って本発明による実施例を詳細に説明する。図２は実施例の暗号処理ＬＳＩＣのブロック図で、図において２０は移動通信端末に組み込まれた実施例の暗号処理ＬＳＩＣ、１１はＮＴＴのＦＥＡＬ－８暗号アルゴリズムに従う鍵処理部、１２はセレクタ部、１３はメモリ部（図１の１に相当）、１４は同ＦＥＡＬ－８暗号アルゴリズムに従うデータランダム化部、１５はトライステートのバッファ回路（同２に相当）、８は秘密鍵保護部（同３～５に相当）である。

【００１６】通常の動作モードでは、テストモード信号ＴＭはＬＯＷレベルであり、これによってセレクタ部１２は入力端子のＡ側を選択し、かつバッファ回路１５の出力ＴＰはハイインピーダンスである。この状態で、予め、基地局からは６４ビット長の鍵データＫＤが秘密に送られる。鍵処理部１１は、この鍵データＫＤをＦＥＡＬ－８暗号アルゴリズムに従って混ぜ合わせることで暗号強度を増した２５６ビット長の拡大鍵データＥＫＤを生成し、これをメモリ部１３に格納する。

【００１７】次に、基地局又は移動通信端末内の不図示のＣＰＵから６４ビット長の平文データＭＤが送られる。データランダム化部１４は、この平文データＭＤとメモリ部１３の拡大鍵データＥＫＤとをＦＥＡＬ－８暗号アルゴリズムに従って混ぜ合わせることでさらに暗号強度を増した暗号データＣＤを生成し、これを外部に出力する。そして、図示しないが、外部においてサンプリング量子化された音声データは、データランダム化部１４の暗号データＣＤによって暗号化され、無線送信される。

5

【００１８】またテストモードでは、テストモード信号ＴＭはＨＩＧＨレベルであり、これによりセレクタ部１２は入力端子のＢ側を選択し、かつバッファ回路１５は後述の秘密鍵保護部８の制御信号Ｓによって制御されることになる。図３は実施例の秘密鍵保護部のブロック図で、図において８１，８２はデコーダ、８３はラッチ回路、８４はＡＮＤ－ＯＲゲート回路から成る比較部、８５は遅延インバータ素子、８６，８７はＡＮＤゲート回路である。なお、デコーダ８１及びラッチ回路８３は図１の記憶部３に相当し、デコーダ８２は同ゲート部５に相当し、比較部８４は同比較部４に相当する。

【００１９】テストモード信号ＴＭが投入されると、その立ち上がり部分を遅延インバータ素子８５及びＡＮＤゲート回路８６で抽出したエッジ信号ＥＴＭが発生し、これによりラッチ回路８３の全出力Q_0 ～Q_n がリセットされる。そして、その後にメモリ部１に対して何らかのテストデータの書き込みが行われると、その際の書込イネーブル信号ＷＥによってその際の書込アドレスＡＤＤをデコードした信号A_0 ～A_n の何れか一つが発生し、これがラッチ回路８３の対応するビットをセットする。こうして、メモリ部１の任意アドレスＡＤＤに任意データＤＡＴＡを書き込むことが可能であり、各書込毎にその書込アドレスＡＤＤをデコードした信号A_0 ～A_n の何れか一つが発生し、これがラッチ回路８３の対応するビットをセットする。

【００２０】また、メモリ部１に対してデータの読み出しを行うと、デコーダ８２はその際の読出イネーブル信号ＲＥによってその際の読出アドレスＡＤＤをデコードした信号A_0 ～A_n の何れか一つを発生する。この状態で、比較部８４はラッチ回路８３の出力信号Q_0 ～Q_n とデコーダ８２の出力信号A_0 ～A_n との各ＡＮＤ－ＯＲ論理をとっている。

【００２１】例えば、今、デコーダ８２の出力信号A_0 がＨＩＧＨレベルの時に、ラッチ回路８３の出力信号Q_0 がＨＩＧＨレベルの時は、このアドレスについては既にテストデータの書き込みが行われており、比較部８４はＨＩＧＨレベルを出力する。また、デコーダ８２の出力信号A_n がＨＩＧＨレベルの時に、ラッチ回路８３の出力信号Q_n がＬＯＷレベルの時は、このアドレスについては未だテストデータの書き込みが行われておらず、

6

比較部８４はＬＯＷレベルを出力する。

【００２２】そして、ＡＮＤゲート回路８７にはテストモード信号ＴＭが入力しているので、結局、秘密鍵保護部８はテストモードでかつ比較部８４の比較一致が得られた時のみＨＩＧＨレベルの制御信号Ｓを出力し、バッファ回路１５は制御信号ＳがＨＩＧＨレベルの時のみメモリ部１の読出データを外部端子ＴＰに出力する。なお、上記実施例では暗号処理ＬＳＩＣを移動通信端末に組み込んだ場合を示したが、他のいかなる暗号処理装置にも適用可能である。

【００２３】また、上記実施例ではＮＴＴのＦＥＡＬ－８暗号アルゴリズムに従う暗号処理を示したが、他の暗号アルゴリズムに従う暗号処理にも適用可能である。

【００２４】

【発明の効果】以上述べた如く本発明によれば、メモリ部１の読出データの外部への出力可否を制御する制御部２と、テストモード信号ＴＭの投入により全記憶情報がリセットされて、その後のメモリ部１へのデータの書き込みを行ったアドレスに係る情報を記憶する記憶部３と、記憶部３の記憶情報とメモリ部１のデータの読み出しを行うアドレスに係る情報とを比較する比較部４とを備え、テストモードでかつ比較部４の比較一致が得られたことにより制御部２を出力可にするので、外部からメモリ部１の読み／書き検査が可能であると共に、外部からは秘密の鍵データを観測することはできない。従って、秘密鍵の盗難による悪用を防止することができる。

【図面の簡単な説明】

【図１】図１は本発明の原理的構成図である。

【図２】図２は実施例の暗号処理ＬＳＩＣのブロック図である。

【図３】図３は実施例の秘密鍵保護部のブロック図である。

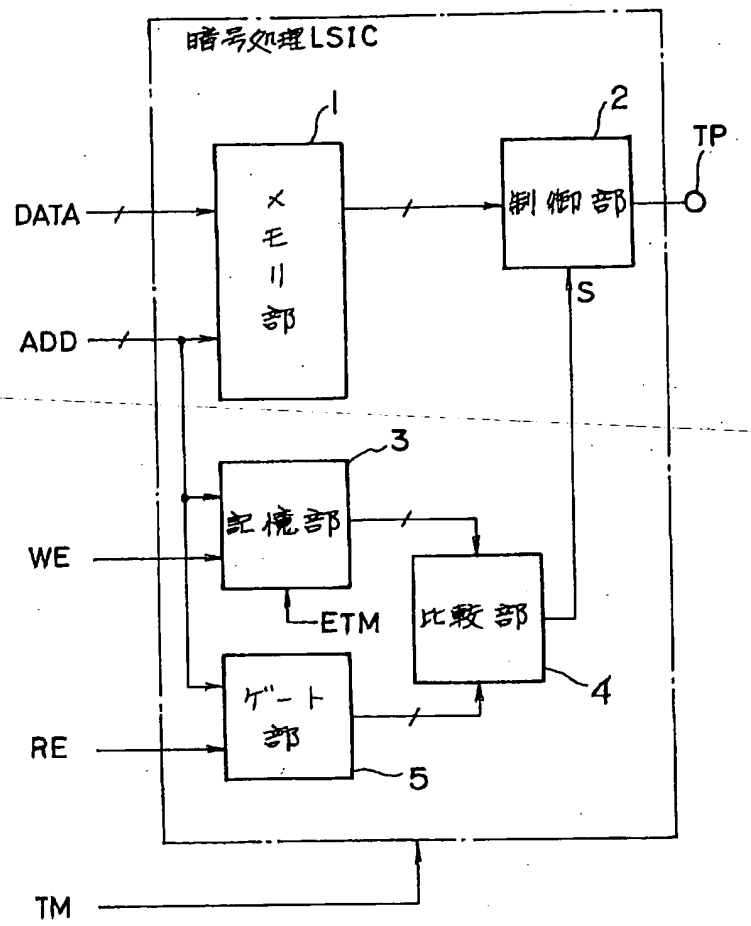
【図４】図４は従来の暗号処理ＬＳＩＣのブロック図である。

【符号の説明】

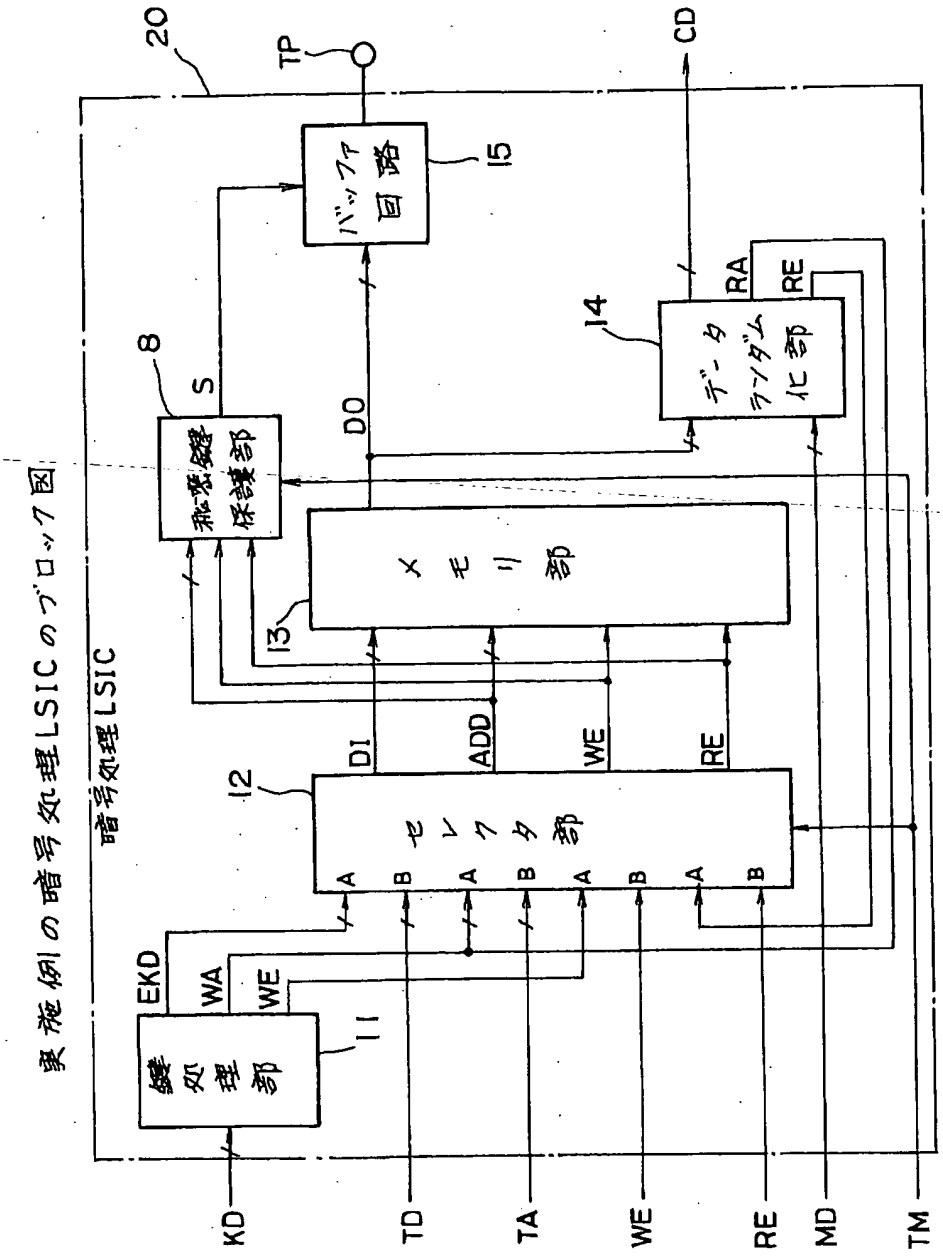
１　メモリ部
２　制御部
３　記憶部
４　比較部
５　ゲート部

【図1】

本発明の原理的構成図

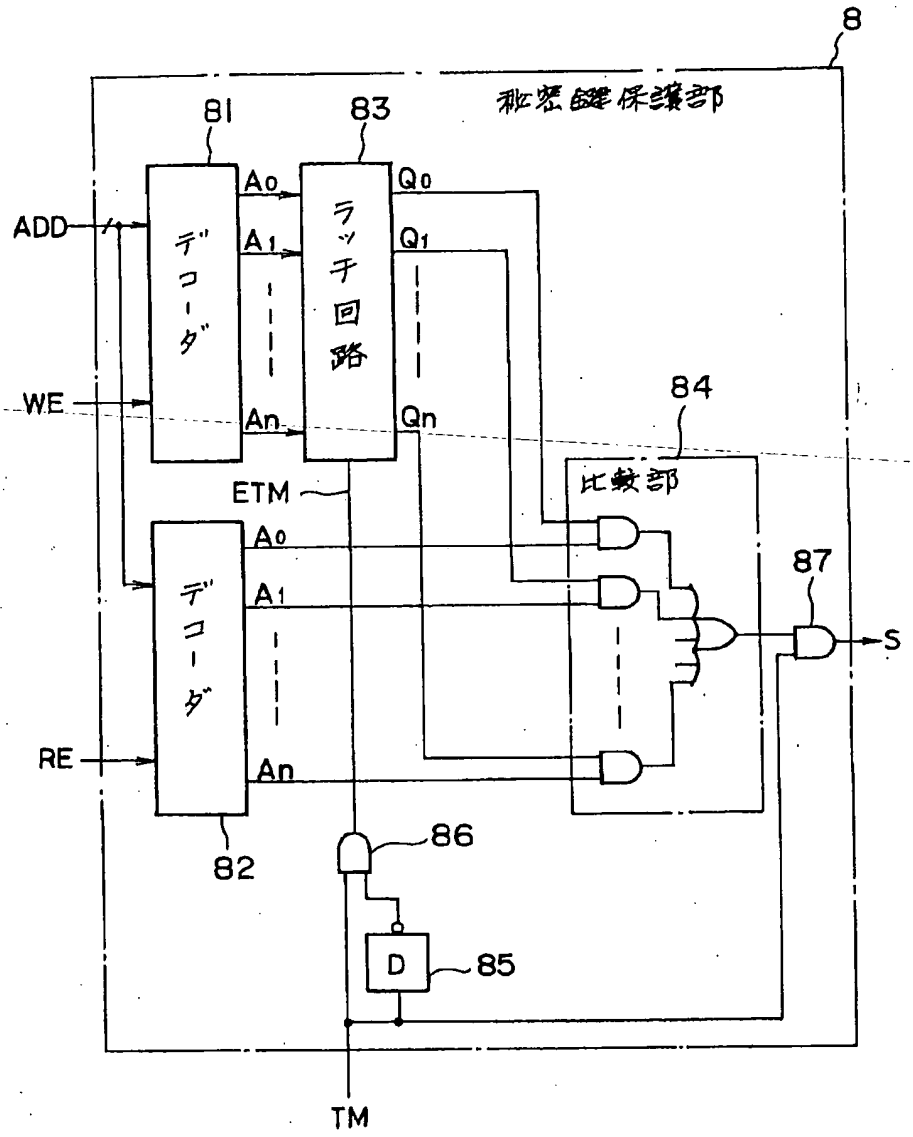


【図2】


20
TP
CD
バッファ回路
15
RA
RE
14
データラッチ化部
8
S
秘密鍵保護部
DO
メモリ部
13
D1
ADD
WE
RE
12
セレクタ部
A
B
EKD
WA
WE
鍵処理部
11
KD
TD
TA
WE
RE
MD
TM
暗号処理LSIC
実施例の暗号処理LSICのブロック図

【図3】

実施例の秘密鍵保護部のブロック図



【図4】

従来の暗号処理LSICのブロック図